Various Notes

Jakob Schneider

September 17, 2014

1 Grundlagen

Zunächst führen wir den Begriff der Gruppe nocheinmal ein

Definition 0.1 (Gruppe). Eine Gruppe G ist eine Struktur $\mathbf{Grp} = \langle \circ, ^{-1}, 1 \rangle$

2 Permutationsgruppen und lineare Gruppen

1 Primitive und mehrfach transitive Permutationsgruppen

2 ...

3 Primitive Permutationsgruppen mit abelschen Normalteilern

Lemma 0.1. *Sei A abelsche transitive Untergruppe von $\operatorname{Aut}\Omega$ ($\Omega : \mathbf{Set}$), dann ist der Zentralisator von A in $\operatorname{Aut}\Omega$ gleich A selbst und A agiert regulär auf Ω.*

Proof. Da A abelsch ist, gilt $A \rightarrowtail \leftarrow \leftarrow \leftarrow \operatorname{C}_{\operatorname{Aut}\Omega} A$. Weiterhin stellt man fest, dass $\operatorname{C}A$ frei agiert, denn falls für $c \in \operatorname{C}A$ gilt $\omega^c = \omega$ für ein $\omega \in \Omega$, dann folgt für $\rho \in \Omega$ wegen Transitivität von A die Existenz eines $a \in A$ mit $\omega^a = \rho$, also $\rho^c = \omega^{ac} = \omega^{ca} = \rho$. Also $c = 1_{\operatorname{Aut}\Omega}$. Damit folgt, dass $\operatorname{C}A$ sowohl transitiv (da A transitiv agiert), als auch frei agiert. Somit $A = \operatorname{C}A$, denn für ein Element $c \in \operatorname{C}A$ mit $\omega^c = \rho$ gibt es mindestens ein $a \in A$ mit derselben Eigenschaft, dann gilt aber $a = c$, wegen Freiheit. □

Lemma 0.2 (Struktur charakteristisch einfacher Gruppen). *Sei G charakteristisch einfach mit minimalem Normalteiler N. Dann ist $G \cong N^{\prod \kappa}$.*

Proof. Betrachte das orbit $O \coloneqq \operatorname{orb}_{\operatorname{Aut} G} N$ von N unter Automorphismen von G. Die davon erzeugt Gruppe $H \coloneqq \langle O \rangle$ liegt charakteristisch in G und $1 < N \geq H$ zeigt $H = G$. Weiterhin schneiden sich je zwei veschiedene Elemente $N_1, N_2 \in O$ trivial, also $[N_1, N_2] \leq N_1 \wedge N_2 = 1$. Damit ist G eine Potenz von N. Zu zeigen bleibt noch, dass N einfach ist. Jeder Normalteiler von N ist aber auch ein Normalteiler von G (da G Potenz von N ist), also folgt, wegen

Minimalität von N, dass ein solcher entweder 1 oder N selbst ist, also ist N einfach. □

Theorem 0.1 (Galois). *Sei G eine Gruppe mit primitiver Aktion auf Ω mit minimalem Normalteiler N. Ist N auflösbar, so gilt:*

(I) *N agiert regulär und ist elementar-abelsch.*

(II) *$G = N\mathrm{stab}_G\omega$ für jedes $\omega \in \Omega$ und $N \wedge \mathrm{stab}_G\omega = 1$.*

(III) *N ist der einzige minimale Normalteiler.*

(IV) *$\mathrm{stab}_G\omega$ hat keine p-Gruppe als Normalteiler.*

(V) *Ist G auflösbar, so sind alle Komplemente von N konjugiert zueinander in G.*

3 Hallo

4 Complex analysis

1 Hallo

$$\sum_{i=1}^{4} 3$$

Lemma 0.3. *Let $(a_n)_{n\in\mathbb{N}}$ be a sequences of non-negative numbers such that*

$$\rho_a := \frac{1}{\limsup_{n\to\infty} \sqrt[n]{a_n}}$$

prove that the sequence $b_n := \sum_{m\geq n} \binom{m}{n} a_m$ satisfies

$$\rho_b \geq \rho_a - 1.$$

Proof. For N sufficiently large we have that $a_n \leq (\rho_a - \varepsilon)^{-n}$ for $n \geq N$. Thus

$$b_n \leq \sum_{m\geq n} \binom{m}{n} (\rho_a - \varepsilon)^{-m} = \left(\frac{1}{1 - (\rho_a - \varepsilon)^{-1}}\right)^{n+1} (\rho_a - \varepsilon)^{-n}$$

by the formula $\left(\frac{1}{1-x}\right)^n = \sum_{i=0}^{\infty} \binom{n-1+i}{n-1} x^i$. Thus

$$\limsup_{n\to\infty} \sqrt[n]{b_n} \leq \frac{1}{(\rho_a - \varepsilon) - 1}$$

for all $\varepsilon > 0$ so $\rho_b \geq \rho_a - 1$. □

Remark 1. The transformation $a_n = \sum_{m\geq n} \binom{m}{n} b_m$ has inverse $(-1)^n b_n = \sum_{m\geq n} \binom{m}{n} (-1)^m a_m$.

Lemma 0.4. *Let $(a_n)_{n\in\mathbb{N}}$ be a sequence of complex numbers such that $\sum_{n\in\mathbb{N}} a_n x^n$ has radius of convergence ρ_a. Then the sequence $(b_n)_{n\in\mathbb{N}}$ defined by the formal equality $\sum_{n\in\mathbb{N}} a_n x^n = \sum_{n\in\mathbb{N}} b_n (x-x_0)^n$ has radius of convergence ρ_b with $|\rho_a - \rho_b| \leq |x_0|$.*

Proof. It is easy to check that b_n is defined by

$$a_n = \sum_{m\geq n} \binom{m}{n} b_m (-x_0)^{m-n} = (-x_0)^{-n} \sum_{m\geq n} \binom{m}{n} \left(\frac{b_m}{-x_0}\right)^m.$$

Thus the previous lemma gives that the radii of convergence ρ'_a and ρ'_b of the sequences $\left(\frac{a_n}{-x_0}\right)_{i\in\mathbb{N}}$ and $\left(\frac{b_n}{-x_0}\right)_{i\in\mathbb{N}}$ satisfy

$$\rho'_a \leq \rho'_b - 1$$

and of course the symmetric identity does also hold (by a change of coordinates). Thus $|\rho'_a - \rho'_b| = \frac{|\rho_a - \rho_b|}{|x_0|} \leq 1$ proving the claim. □

5 Filtered spaces

$$\bullet_1 \to_a \bullet_2 \operatorname{End}_A A$$

Definition 0.2 (antitone Galois connection of convergent nets and filters). Let X be a space with convergence structure C (i.e. a bunch of convergent nets in X). Then define

$$\mathrm{N}_x\mathrm{C} \coloneqq \left\{N \in \operatorname{Sub} X : \forall\, (x_i)_{i\in I} \in \mathrm{C}_x : \exists i \in I : \forall j \geq i : x_i \in N\right\}$$

and analogously for a given filter system N define

$$\mathrm{C}_x\mathrm{N} \coloneqq \left\{(x_i)_{i\in I} \in I \to X : \forall N \in \mathrm{N}_x : \exists i \in I : \forall j \geq i : x_i \in N\right\}.$$

Then the above operators form an antintone Galois connection.

Definition 0.3. A filtered space X is a structure with operators N such that each $x \in X$ gets assigned to a filter $\mathrm{N}|_x X$ which is a subset of $\operatorname{Sub} X$, where any filter element contains x.

Definition 0.4 (ordered sets as filtered spaces). Ordered sets are filtered spaces in a natural way. For $x \in X$ the filter $N|_x X$ is defined as the filter generated by all sets of the form $X \setminus [y)$ where $y \not\leq x$.

6 Filters and convergence

A filtered space can be discribed either by its filters or its convergent nets.

7 Lattices and posets

Definition 0.5 (topology of complete lattices). A complete lattice admits a natural filter stucture which is generated by the convergence of monotone nets. This filter structure is said to be the filter structure induced by the order of L.

Lemma 0.5. *For $x \in X$ by the previous definition the filter in x is*

$$\mathrm{N}_x X \coloneqq \mathrm{N}_x^\vee X \cup \mathrm{N}_x^\wedge X$$

where

$$\mathrm{N}_x^\vee X \coloneqq \left\{ U \in \operatorname{Sub} X : \forall (x_i)_{i\in I} : \left(\bigvee_{i\in I} x_i = x \wedge \forall i, j : i \leq j \Rightarrow x_i \leq x_j \right) \Rightarrow \exists i \in I : \forall j \geq i : x_j \in U \right\}$$

and

$$\mathrm{N}_x^\wedge X \coloneqq \left\{ U \in \operatorname{Sub} X : \forall (x_i)_{i\in I} : \left(\bigwedge_{i\in I} x_i = x \wedge \forall i, j : i \leq j \Rightarrow x_i \geq x_j \right) \Rightarrow \exists i \in I : \forall j \geq i : x_j \in U \right\}.$$

Moreover, $\mathrm{N}_x^\vee$ is generated by the complements of lower-closed $\bigvee$-closed sets containing x and dually, $\mathrm{N}_x^\wedge$ is generated by the complements of upper-closed $\bigwedge$-closed sets.

Proof.

Lower-open $\bigvee$-open sets are in $\mathbf{N}_{\boldsymbol{x}}^\vee \boldsymbol{X}$. Let $(x_i)_{i\in I}$ be a non-decreasing net with $\bigvee_{i\in I} x_i = x$ and C be a lower-closed $\bigvee$-closed set not containing x. Assuming that $x_i \in C$ for all $i \in I$ leads to $\bigvee_{i\in I} x_i = x \in C$ since C is $\bigvee$-closed, a contradiction. Thus $x_i \in X \setminus C$ for some $i \in I$. Since C is lower-closed it follows that $x_j \in X \setminus C$ for all $j \geq i$ (since otherwise $x_i \in C$, a contradiction).

Lower-open $\bigvee$-open sets generate $\mathbf{N}_{\boldsymbol{x}}^\vee \boldsymbol{X}$. To show that these sets generate $\mathrm{N}_x^\vee X$ we pick a non-decreasing net $(x_i)_{i\in I}$ with $\bigvee_{i\in I} x_i = x$. We have to show that the filter generated by these sets says that $(x_i)_{i\in I}$ converges. For each $y \not\geq x$ the set $(y]$ is lower-closed and $\bigvee$-closed. Thus a limit x' of $(x_i)_{i\in I}$ with respect to the filter generated by the lower-open $\bigvee$-open sets then must also lie outside $(y]$. Then $x' \not\leq y$ for $y \not\geq x$. But then $x' \geq x$ since otherwise $x' \not\geq x$ and $x \leq x$ a contradiction.

Conversely, we deduce that any $x' \in x^\wedge$ is a limit in the second sense.

Dually, we are done. □

Definition 0.6 (completion lattice of a poset).

Definition 0.7 (upper and lower bounds for posets). For a set $A \subseteq P$ write

$$A^\vee \coloneqq \{p \in P : \forall a \in A : a \leq p\}$$

for the set of upper bounds of A and

$$A^\wedge \coloneqq \{p \in P : \forall a \in A : p \leq a\}$$

for the set of lower bounds. These operators correspond to the operators $\bigwedge$ and $\bigvee$ of the completion lattice of P in the sense that when $\iota : P \to \overline{P}$ is the canonical map to the completion lattice then $\bigvee \operatorname{Sub}(\iota)(A^\wedge) = \bigwedge \operatorname{Sub}(\iota)(A)$. Moreover, the operators $\wedge$ and $\vee$ form an antitone Galois connections $\langle\langle \operatorname{Sub}(P), \wedge\rangle, \langle \operatorname{Sub}(P), \vee\rangle\rangle$

on the subsets of the poset P similarly as $\bigwedge$ and $\bigvee$ form such connection on the subsets of a complete lattice.

Definition 0.8 (topology of posets). A poset P is equipped with a natural topology which is induced by the GALOIS connection $\langle\langle \mathrm{Sub}(P), \wedge\rangle, \langle \mathrm{Sub}(P), \vee\rangle\rangle$ when defining the closed sets to be the GALOIS closed sets. It can be descibed by

$$\tau_P := \langle P \setminus A^{\wedge}, P \setminus A^{\vee} : A \in \mathrm{Sub}(P)\rangle.$$

Remark 2. Here closed intervals are already closed under intersection since it holds for antitone GALOIS-connections that

$$\bigcap_{i\in I} A_i^{\wedge} = \left(\bigcup_{i\in I} A_i\right)^{\wedge} \text{ and } \bigcap_{i\in I} A_i^{\vee} = \left(\bigcup_{i\in I} A_i\right)^{\vee}.$$

// analogue between complete lattice and PID

Lemma 0.6 (bounds for the limit point of a sequence). *Let $N := (a_i)_{i\in I}$ be a net in a poset P. Then any accumulation point a of N it holds that*

$$a \in \left(\bigcup_{i\in I} \{a_j : j \geq i\}^{\wedge}\right)^{\vee} \cap \left(\bigcap_{i\in I} \{a_j : j \geq i\}^{\vee}\right)^{\wedge}$$

and if P is a complete lattice, this can be written as

$$\bigvee_{i\in I}\bigwedge_{j\geq i} a_j \leq a \leq \bigwedge_{i\in I}\bigvee_{j\geq i} a_j.$$

Proof. It is clear that for $i \in I$ we have $a \in \{a_j : j \geq i\}^{\wedge\vee} \cap \{a_j : j \geq i\}^{\vee\wedge}$ or equivalently for a lattice $\bigwedge \{[\} j \geq i] a_j \leq a \leq \bigvee \{[\} j \geq i] a_j$ since otherwise $P \setminus \{[\} j \geq i] a_j{}^{\vee\wedge}$ or $P \setminus \{[\} j \geq i] a_j{}^{\vee\wedge}$ would be an open neighbourhood of a not containing a point of $\{[\} j \geq i] a_j$ (contradicting the assumption that a is an accumulation point of N). Thus we have that

$$a \in \bigcap_{i\in I} [j \geq i]\{a_j\}^{\wedge\vee} \cap \bigcap_{i\in I} \{[\} j \geq i] a_j{}^{\vee\wedge} = \left(\bigcup_{i\in I} \{[\} j \geq i] a_j{}^{\wedge}\right)^{\vee} \cap \left(\bigcap_{i\in I} \{[\} j \geq i] a_j{}^{\vee}\right)^{\wedge},$$

or respectively for the complete lattice case

$$\bigvee_{i\in I}\bigwedge_{j\geq i} a_j \leq a \leq \bigwedge_{i\in I}\bigvee_{j\geq i} a_j.$$

□

Definition 0.9 (limes superior and inferior). Let $N := (a_i)_{i\in I}$ be a net in a poset P. When there exists elements $\check{N}, \hat{N} \in P$ such that

$$\sup\left(\bigcup_{i\in I} \{[\} j \geq i] a_j{}^{\wedge}\right) = \hat{N}$$

or

$$\inf\left(\bigcup_{i\in I}\{[\}\, j\geq i]a_j{}^{\wedge}\right)=\check{N}$$

then $\hat{N}$ is called *limes superior* and denoted by $\limsup N$ and $\check{N}$ is called *limes inferior* and denoted by $\liminf N$.

Now we introduce the notion of a topological lattice

Definition 0.10 (topological lattice). Let L be a structure the form $\langle L',\tau\rangle$ where $L'=\langle L'',\wedge,\vee,\leq\rangle$ is a lattice and τ is a topology on L' under which $\wedge,\vee: L\sqcap L\to L$ are continuous.

Lemma 0.7. *Let $L=\langle L',\tau\rangle$ be topological lattice with an identifying, separating topology (T_1 space) then τ contains the* Galois *topology of L'. The converse is also true.*

Proof. Let $x\in L$ then since τ is T_1 the set $\{x\}$ is closed. Define $f:=(c_x\wedge \mathrm{id}_L)\vee$ where c_x is the constant map then f is continuous. Thus, $f^{-1}\{x\}=\{x\}^{\vee}$ is closed. This implies that for all $A\subseteq L$ the set $A^{\vee}=\bigcap_{a\in A}\{a\}^{\vee}$ is closed. For $\wedge$ the dual argument works. For the other direction, note that $\{x\}^{\vee}\cap\{x\}^{\wedge}=\{x\}$ is closed in the Galois topology, so L is T_1. □

Lemma 0.8 (monotone nets in posets). *Let P be a poset equipped with* Galois *topology and $N:=(a_i)_{i\in I}$ a monotone net, i.e. $i\leq j$ implies $a_i\leq a_j$. Then it holds that*

(I) If N is non-decreasing $\sup N=\lim N$.

(II) If N is non-increasing $\inf N=\lim N$.

Moreover, N has at most one accumulation point.

Proof. We only prove the first statement, the second following by duality.

Let a an accumulation point of N. Then a is an upper bound of $\{[\}\, i\in I]a_i$ for otherwise there would exist an $i\in I$ such that $a_i\not\leq a$ implying that $P\setminus\{a_i\}^{\vee}$ is a neighbourhood of a not containing a point of $(a_j)_{j\geq i}$ contradicting the assumption that a is an accumulation point of N. Moreover, if there exists an $a'<a$ which is also an upper bound of $\{[\}\, i\in I]a_i$ then $P\setminus\{a'\}^{\wedge}$ is an open neighbourhood of a not containing a point of N. Thus, if $\lim N$ exists it must be the supremum of N. Conversely, if the supremum of N exists, it must be its limit. This can be seen from as follows. Assume there is an open neighbourhood U of $\sup N$ which seperates it from N. Then by reducing to the base of topology of the Galois topology we can assume that $U=P\setminus(\bigcup_{i=1}^{n}A_i^{\wedge}\cup\bigcup_{i=1}^{m}B_i^{\vee})$. When there is an $i\in I$ and $j\in\{1,\dots,m\}$ such that $a_i\in B_j^{\vee}$ then $\sup N\in U$. So we may assume that $m=0$. On the other hand, it is easy to see that the sets $A_i^{\wedge}\cap\{[\}\, i\in I]a_i$ are totally ordered by inclusion since N is non-decreasing. Thus there is an $i\in\{1,\dots,n\}$ such that $\{[\}\, i\in I]a_i\subseteq A_i^{\wedge}$. But then $\sup N\in A_i^{\wedge}$ by definition of the supremum. □

Lemma 0.9 (topology of posets). *A lattice L is a topological space when equipped with the topology $\tau:=\langle\{c\in L: a\not\leq c\not\leq b\}: a,b\in L\rangle$ such that lattice*

convergence and topological convergence coincide.

Proof. Let a net $(a_i)_{i\in I}$ converge in P to a. Then from $a = \limsup_{i\in I} a_i$ we know that for all $a' < a$ there exists an $i \in I$ such that for all $j \geq i$ one of the sets $\{[\} k \geq j]a_k$ has an upper bound u which is smaller than a'. □

2 Rank

Definition 0.11. Let $P : \langle P', 0, \leq\rangle$ be a poset with a distinguished element 0 and $L : \langle L', \wedge, \vee, 0\rangle$ be a complete lattice with a distinguished element 0. A map $\mathrm{rk} : P \to L$ is called a rank function if

(I) $\mathrm{rk}\, 0 = 0$,

(II) $\forall p \in P : \mathrm{rk}\, p = \bigwedge \{q \in P : \forall r < p : q > \mathrm{rk}\, r\} = \bigvee \{q \in P : \forall r > p : q < \mathrm{rk}\, r\}$.

Remark 3. Mostly, P will itself be a lattice. We will however see that rank functions occur in many areas of classical algebra as well as measure theory.

8 Measures

9 Preliminaries

Here, I assemble some notes on various interesting subjects.

Definition 0.12 (preorder). A preorder on a set S is a relation $\leq\subseteq S^{\times 2}$ satisfying the following properties.

(I) *Transitivity* If $a \leq b \leq c$ then $a \leq c$.

(II) *Reflexivity* It holds that $\mathrm{id}_S \subseteq\leq$.

Definition 0.13 (Directedness). A preorder $\leq$ on a set S is called directed if it for all $a, b \in S$ there exists a c such that $a, b \leq c$ (existence of upper bounds for finite sets).

Definition 0.14 (order). An *order* is a identifying or seperating preorder, that is, if $a \leq b$ if and only if $a' \leq b$, and $a \geq b$ if and only if $a' \geq b$ then $a = a'$. More simply, one can weaken this to $a \leq a'$ and $a' \leq a$ implies that $a = a'$.

Remark 4. Think of T_1 spaces.

Definition 0.15 (net). A net N is a structure $\langle I, \leq\rangle$ where $\leq$ a directed preorder.

Definition 0.16 (substructures). For a structure S define the lattice of substructures as $\mathrm{Sub}(S)$ (every lattice is a net).

Definition 0.17 (topological summation). Let A be a topological abelian group. Then define the sum of a set $B \subseteq A$ as

$$\sum B := \lim_{B' \in \mathrm{Sub}_{\mathrm{fin}}(B)} \sum B'.$$

Lemma 0.10 (properties of topological summation).

Proof. Let $(B_i)_{i\in I}$ be a net in $\mathrm{Sub}(A)$ such that $\lim_{i\in I} B_i = B$. □

Lemma 0.11 (Riesz' rising sun lemma). *Let $f : [a,b] \to \mathbb{R}$ be a continuous function. Define the* set of shadowed points *S by*

$$S := \{x \in [a,b] : \exists y \in [a,b] : y > x \wedge f(y) < f(x)\}. \tag{(1)}$$

Then it holds that

1. *S is open within $[a,b)$.*
2. *If (a',b') is a maximal open interval within S then*
   (a) *$f(a') = f(b')$ if $a' \neq a$.*
   (b) *$f(a') \leq f(b')$ if $a' = a$.*
   (c) *$\forall x \in (a',b') : f(x) < f(b')$.*

Proof. The set S can be written as

$$\begin{aligned} S &= \bigcup_{y\in[a,b]} \{x \in [a,b] : x < y \wedge f(x) < f(y)\} \\ &= \bigcup_{y\in[a,b]} (\{x \in [a,b) : x < y\} \cap \{x \in [a,b) : f(x) < f(y)\}) \end{aligned}$$

which is open as a union of finite intersection of open sets. To prove the second claim, let $a', b' \in [a,b]$ such that $(a',b') \subseteq S$ is a maximal open interval (it may happen that also $a' \in S$ if $a' = a$, but $b' \notin S$ as S is open within $[a,b)$). Now, define

$$b'' := \min \left\{ x \in [b',b] : f(x) = \max_{y\in[a',b]} f(y) \right\}. \tag{(2)}$$

(Due to the continuity of f and as $[b',b]$ is compact this minimum exists and equals the infimum of the same set.) We show that $b'' = b'$. Observe that for $x \in [b',b'')$ it holds that $x < b''$ and $f(x) < f(b'')$ from which we deduce that $x \in S$ by the definition of S. Thus it follows that $(a',b') \cup [b',b'') = (a',b'') \subseteq S$ which implies $b'' = b'$ as (a',b') is a maximal open interval within S.

Let $x \in (a',b')$. By the definition of S there exists $y \in (x,b]$ with $f(x) < f(y)$. Now, using the last fact we have that $f(b') = f(b'') > f(y)$ if $y > b'$. Thus, there exists $y \in (x,b']$ such that $f(x) < f(y)$. This shows, that $f|_{[x,b']}$ does not attain its maximum in x. Now let $z \in [x,b']$ such that $f(z) = \max_{y\in[x,b']} f(y)$. Then $f(z) = \max_{y\in[z,b']} f(y)$ from which we deduce that $z = b'$ for if $z \in (a',b')$ would lead to a contradiction by the last fact. Thus $f(x) < f(b')$.

As f is continuous, it follows that $f(a') \leq f(b')$. If $a < a'$ then by the maximality of (a',b') we have that $a' \notin S$ from which we deduce that $f(a') \geq f(b')$ from the above, which gives $f(a') = f(b')$. □

10 Functions and relations

Definition 0.18 (binary relation). Let $A, B \in \mathbf{Set}$. Then we define the *Cartesian product* of A and B as $A \sqcap B = \{(a, b) : a \in A \wedge b \in B\}$. A *binary relation* R between A and B is a subset of $A \sqcap B$.

Remarks.

1. The Cartesian product $A \sqcap B$ is a direct product of A and B in the categorical sense (thus the notation coincides 'up to isomorphism' with the notation for the direct product).
2. Here, the tuple (a, b) is defined as $\{\{a\}, \{a, b\}\}$.
3. For convenience, we abbreviate $(a, b) \in R$ by aRb, $\{a \in A : aRb\}$ by Rb and $\{b \in B : aRb\}$ by aR.

Definition 0.19 (Composition of binary relations). Let $R \subseteq A \sqcap B$ and $S \subseteq B \sqcap C$. Then the composition of R and S is defined as $R \circ S = \{(a, c) \in A \sqcap C : \exists b \in B : aRbSc\}$.

Definition 0.20 (antisymmetric). A binary relation $R \subset A \sqcap A$ is called *antisymmetric* if for $a, b \in A$ we have that aRb and bRa imply $a = b$. For more general relations, we note these relational sets by R_a (stabilizer notation).

Definition 0.21 (identifying or separating relation). A binary relation $R \subset \prod_{i \in I} A_i$ is called *separating* or *identifying* in A_j if an object of A_j is identified by its relational behavior. That is, for $a, b \in A_j$ the equality $\pi_j^{-1}(a) \cap R = \pi_j^{-1}(b) \cap R$ implies $a = b$ where π_j is the projection from the product $\prod_{i \in I} A_i$ onto the j-th factor.

Remarks

1. The notion of separating relations appears in many areas (e.g. Hausdorff-spaces, dual pairings etc.).

Functions $(f(x), x)$ for the correctness of composition.

11 Primitive roots of unity and the Carmichael function

Definition 0.22 (Exponent of a group). The exponent $\exp(G)$ of some group G is defined as the smallest number $n \in \mathbb{N}$ such that for all $g \in G$ we have $g^n = \mathrm{id}_G$. If such number does not exist, say the exponent of G is infinity ($\exp(G) = \infty$).

Lemma 0.12. *If G is an abelian group then $\{\mathrm{ord}(g) : g \in G, \mathrm{ord}(G) < \infty\}$ (here g runs over the torsion module of the $\mathbb{Z}$-module G) is a sublattice of $\mathbb{Z}$ (equipped with the devided-by relation). Moreover, $\exp(G) = \bigvee_{g \in G} \mathrm{ord}(g)$.*

Proof. Let $a, b \in G$. We have to show that there exists an element $c \in G$ with $\mathrm{ord}(c) = a \vee b$. As $\mathbb{Z}$ is a PID we have numbers $a', b' \in \mathbb{Z}$ such that

$\operatorname{ord}(a) \wedge \operatorname{ord}(b) = a' \operatorname{ord}(a) + b' \operatorname{ord}(b)$. Thus $c := b'a + a'b \in G$ (interpreting G as a $\mathbb{Z}$-module) is an element of the desired order which can be seen from the homomorphism $\phi : \langle c \rangle \to \langle a \rangle \sqcap \langle b \rangle$ via $x \mapsto (\operatorname{ord}(b)x, \operatorname{ord}(a)x)$ and the first homomorphism theorem. At first we see that $\operatorname{ord}(b)c = b' ord(b)a \in \langle a \rangle$ and $\operatorname{ord}(a)c = a' \operatorname{ord}(a)b \in \langle b \rangle$ showing that the domains are correct. Moreover, we have that $\phi(kc) = k\phi(c) = k(b' \operatorname{ord}(b)a, a' \operatorname{ord}(a)b) = 0$ if and only if $k \operatorname{ord}(b) = 0 \bmod \operatorname{ord}(a)$ and $k \operatorname{ord}(a) = 0 \bmod \operatorname{ord}(b)$. But this equivalent to $k = 0 \bmod \operatorname{ord}(a) \vee \operatorname{ord}(b)$. Thus we see that $\langle c \rangle \cong \mathbb{Z}_{\frac{\operatorname{ord}(a)}{\operatorname{ord}(a) \wedge \operatorname{ord}(b)}} \sqcap \mathbb{Z}_{\frac{\operatorname{ord}(a)}{\operatorname{ord}(a) \wedge \operatorname{ord}(b)}} \cong \mathbb{Z}_{\operatorname{ord}(a) \vee \operatorname{ord}(b)}$. □

Lemma 0.13. *Let p be prime, $k \geq 1$ and $a \in \mathbb{Z}^*_{p^{k+1}}$ be such that its projection $\overline{a} \in \mathbb{Z}^*_{p^k}$ is an element of maximum order. Then the $\operatorname{ord}_{\mathbb{Z}^*_{p^{k+1}}}(a) \in \left\{ \operatorname{ord}_{\mathbb{Z}^*_{p^k}}(\overline{a}), p \operatorname{ord}_{\mathbb{Z}^*_{p^k}}(\overline{a}) \right\}$.*

Proof. It is clear that $\operatorname{ord}_{\mathbb{Z}_{p^{k-1}}}(\overline{a}) | \operatorname{ord}_{\mathbb{Z}_{p^k}}(a)$ as $a^n = 1 \Rightarrow \overline{a}^n = \overline{1}$. Moreover, since $\mathbb{Z}_p$ is a field $\mathbb{Z}^*_p$ is cyclic and thus $p - 1 | \operatorname{ord}(\overline{a}) | \operatorname{ord}(a)$ (as $\mathbb{Z}_p$ is a quotient ring of $\mathbb{Z}_{p^{k-1}}$). Thus we have that $\operatorname{ord}(\overline{a}) = (p-1)p^j$ for some $j \leq k$ as $\operatorname{ord}(\overline{a}) | \phi(p^k) = (p-1)p^{k-1}$. Finally, we have that $a^{p \operatorname{ord}(\overline{a})} \in (\langle p^{k-1} \rangle_{\mathrm{Con}} + 1)^p = \{1\}$ which completes the proof. □

Proof. Let $a \in \mathbb{Z}$ such that $\operatorname{ord}(a) \bmod \mathbb{Z}^*_{p^k}$ is maximal. ... □

12 fields

Lemma 0.14. *Let K be a connected ordered field (where the topology is the induced order topology). Then $K \cong \mathbb{R}$.*

Proof. Consider $R \coloneqq \operatorname{cl} \mathbb{Q}$. Then R is closed by definition. On the other hand, R is closed, since any element $k \in K$ satisfying $\mathbb{Q} \leq k$ or $k \leq \mathbb{Q}$ has the open neighbourhood $N \coloneqq (-1 + k, k + 1)$ satisfying $\mathbb{Q} < N$ or $N < \mathbb{Q}$ implying that $k \notin R$. So any $r \in R$ must lie between two rationals. But then $R = \bigcup_{n \in \mathbb{N}} (-n, n)$ is open. But K is connected and $R \neq \emptyset$ so $K = R$. On the other hand, it is clear that the supremum of any open interval must exist in R since otherwise one could find a non-trivial decomposition of R. Thus $R \cong \mathbb{R}$. □

Exercise 0.1. Prove that the following two are equivalent in some field F.

(I) Every polynomial function is surjective.

(II) F is algebraically closed.

Solution. Trivial.

Exercise 0.2. Let A be an algebra and $\operatorname{End} A$ its endomorphisms. Prove that if $\operatorname{Out} \operatorname{Aut} A \cong 1$ then $\operatorname{Aut} \operatorname{End} A = \operatorname{Aut} A$.

Solution. Clearly, $\operatorname{Aut}(A)$ embeds in $\operatorname{Aut} \operatorname{End} A$ via the map $\iota : \operatorname{Aut} A \to \operatorname{Aut} \operatorname{End} A$ by $\iota(\alpha)(\phi) = \alpha^{-1} \phi \alpha$. On the other hand, for any $\beta \in \operatorname{Aut} \operatorname{End} A$ we

have that $\beta|_{\operatorname{Aut} A} \in \operatorname{Aut}\operatorname{Aut} A$ and as $\operatorname{Out}\operatorname{Aut} A \Leftrightarrow 1$ any automorphism is a conjugation.

??

Lemma 0.15 (subfields of fractional field). *Let $\alpha = \frac{P}{Q} \in K(X)$ for some field K and polynomials $P, Q \in K[X]$ then $[K(X) : K(\alpha)] = \max\{\deg_X P, \deg_X Q\}$.*

Proof. Set $R(Y) = P(Y) - \alpha Q(Y)$ then $R(X) = 0$ and R is irreducible in $K(\alpha)[Y]$ since it is irreducible in $K[\alpha][Y] = K[Y][\alpha]$ as a linear polynomial (Gauss Lemma). □

Exercise 0.3. Prove that $\operatorname{Aut}(K(X)/K) \Leftrightarrow \operatorname{GL}[K^2]$

Solution. Let us first notice that all $\alpha = \frac{aX+b}{dX+c}$ with $ac - bd \neq 0$ induce field automorphisms since

$$\alpha \circ \alpha' = \frac{a\frac{a'X+b'}{c'X+d'} + b}{c\frac{a'X+b'}{c'X+d'} + d} = \frac{(aa' + bc')X + (ab' + bd')}{(ca' + dc')X + (cb' + dd')}$$

for appropriate α, α' showing that these α form a group isomorphic to $\operatorname{GL}[K^2]$. Any K-endomorphism α of $K(X)$ is uniquely determined by its image on X thus we may assume that $\alpha(X)$ is some rational function such that there is a rational function β with $\beta \circ \alpha(X) = X$ if α is left invertible (and an automorphism has both left and right inverse). This implies that α interpreted as a map on an algebraic closure $\overline{K} \cup \{\infty\}$ of K is injective. Let $\alpha = \frac{P}{Q}$. W.l.o.g. we may assume that $\deg_X P \geq \deg_X Q$ and that P, Q are monic since if α has left inverse β then $1/\alpha$ has left inverse $1/\beta$ and $c\alpha(X)$ has left inverse $\beta(c^{-1}X)$. Injectivity of α means that $\alpha(z) = c$ has only one solution $z \in \overline{K} \cup \{\infty\}$ for $c \in \overline{K} \cup \{\infty\}$ or equivalently $P - cQ$ is completely inseparable. For all but one $c = -1$ if $\deg_X P = \deg_X Q$ all these polynomials are monic and have degree $d := \deg_X P$. Assume first that $\deg_X P > \deg_X Q$. Thus plugging in two of these c (they exist since $\overline{K}$ is infinite) with difference one gives that

$$Q = (X - \xi)^d - (X - \xi')^d = \sum_{i=1}^{d} (-1)^i \binom{d}{i} (\xi^i + \xi'^i) X^{n-i}$$

But on the other hand Q must itself be inseparable so

$$\sum_{i=1}^{d} (-1)^i \binom{d}{i} (\xi^i + \xi'^i) X^{n-i} = c_Q (X - \xi'')^{d-1}$$

from which we get

$$(-1)^i \binom{d}{i} (\xi^i + \xi'^i) = c_Q \binom{d-1}{i-1} (-1)^{i-1} \xi''^{i-1}$$

Similarly, since if α is left invertible then also $1/\alpha$ (inverse is $1/\beta$). Thus $P = c_P(X - \xi_P)^n$, $Q = c_Q(X - \xi_Q)^m$ for some $c_P, c_Q \in K$, $\xi_P, \xi_Q \in \overline{K}$, $m, n \in \mathbb{N}$.

Exercise 0.4. Let $f : K \to K$ be a mapping where K is a field with subfield $L \leq K$. Assume that

$$f(\alpha x + \beta y) = \alpha f(x) + \beta f(y)$$

for all $\alpha, \beta \in L$ and $x, y \in K$ (that is f is L-linear) and additionaly that

$$f(x)f(1/x) = 1$$

for $x \in K^*$ and $f(1) = 1$. Show that $f \circ F = F \circ f$ for any L-rational function $F \in L(X)$. Moreover, show that $f \in \mathrm{End}(K/L)$ if $\mathrm{char}\,(K) \neq 2$. Deduce that $f \in \mathrm{Aut}(K/L)$ in the case where K/L is algebraic and that $f = \mathrm{id}$ in the case $K = \mathbb{R}$, $L = \mathbb{Q}$.

Solution of Exercise 0.4arabic11. At first we show that $f(x^n) = f(x)^n$ for all $n \in \mathbb{N}$. This can be seen by induction from $f(x^1) = f(x)^1$ and the induction step

$$\begin{aligned} f\left(\frac{1}{x} - \sum_{i=1}^{n} \frac{1}{(1+x)^n}\right) &= f\left(\frac{1}{x(1+x)^n}\right) \\ &= \frac{1}{f(x)(1+f(x))^n - f(x)^{n+1} + f(x^{n+1})} \\ &= \frac{1}{f(x)} - \sum_{i=1}^{n} \frac{1}{(1+f(x))^n} \end{aligned}$$

where we deduce that $f(x^{n+1}) = f(x)^{n+1}$ for $x \in K \setminus \{0, -1\}$ from $f(x^k) = f(x)^k$ for all $1 \leq k \leq n$. But obviously $f(0) = 0$ and $f(-1) = -1$ can be derived from the additivity of f and from $f(1) = 1$. If $\mathrm{char}\, K \neq 2$ we then get $f((x+y)^2) = f(x)^2 + f(y)^2 + 2f(x)f(y) = f(x^2) + f(y^2) + 2f(xy)$ implying that $f(xy) = f(x)f(y)$. Thus $f \in \mathrm{End}(K/L)$ as $f(x) = x$ for $x \in L$ (by L-linearity). If K is algebraic over L then $\mathrm{Aut}(K/L) = \mathrm{End}(K/L)$ proving the second fact in the case $\mathrm{char}\, K \neq 2$. On the other hand, the multiplicativity of f follows as well for $\mathrm{char}\, K = 2$ and L/K finite. Thus it also holds for the inductive limit of finite field-extensions. In the case $K = \mathbb{R}$ we get that $f(x)^2 = f(x^2)$ showing that f is continuous and thus $f(x) = x$.

Exercise 0.5. Determine the minimum number of 3-cylces necessary to generate A_n.

Solution of Exercise 0.5arabic12. It is clear that for $n \geq 3$ as A_n acts transitively. Let $\langle c_i : i \in I \rangle = A_n$ where c_i are the 3-cycles. Then for $n \geq 4$ the following condition must be satisfied by the c_i $(i \in I)$ for otherwise $\langle c_i : i \in I \rangle$ would not be transitive.

For all subsets $I' \leq I$ such that $M := \bigcup_{i \in I'} \mathrm{spt}\, c_i \subset n$ there exists $j \in I \setminus I'$ such that $\mathrm{spt}\, c_j \cap M \neq \emptyset$ and $\mathrm{spt}\, c_j \not\subseteq M$.

This implies inductively that $\left|\bigcap_{i \in I'} \mathrm{spt}\, c_i\right| \leq 3 + 2(i-1)$. Thus it follows that $1 + 2\,|I| \geq n$ must hold. We claim that any set $\{c_i : i \in I\}$ satisfying the above condition necessary for transitity of the action of $\langle c_i : i \in I \rangle$ generates A_n.

Case 1. To prove this we first assume that there are two 3-cycles intersecting in only one point. That is w.l.o.g. $\alpha := c_1 = (1\ 2\ 3)$ and $\beta := c_2 = (3\ 4\ 5)$. Then one computes that $\gamma := \left[\alpha, \beta^{-1}\right] = (2\ 3\ 4)$. Thus the induction hypothesis gives that $\langle c_i : i \in I\rangle \geq \langle c_i, \gamma : i \in I \setminus \{1\}\rangle \geq \mathrm{stab}_{A_n}(1) \Leftrightarrow A_{n-1}$. But the point stabilizer of a primitive action is a maximal subgroup and $\langle c_i : i \in I\rangle$ contains c_1 not fixing 1. Thus in this case we are done.

Case 2. In this case we may assume that all cycles c_i are of the form $c_i = (1\ 2\ (i+2))$ for $i = 1, \ldots, n-2$. But again we see that $\langle c_i : i = 1, \ldots, n-2\rangle \geq \langle c_i : i = 1, \ldots, n-3\rangle = \mathrm{stab}_{A_n}(n) \Leftrightarrow A_{n-1}$ by induction hypothesis. Again $\langle c_i : i \in I\rangle$ contains a point stabilizer and an element c_n not in this stabilizer. Thus it is A_n again.

13 Group theory

3 The p-Sylow theorem

Theorem 0.2 (number of p^e-subgroups). *Let G be a finite group of order $|G| = n = mp^e$ and let $p^e | n$ for some prime p and $m, e \in \mathbb{N}$. Then the set of subgroups $S_{p^e} := \{P \leq G : |P| = p^e\}$ satisfies*

$$|S_{p^e}(G)| \quad = \tfrac{1}{m}\tbinom{n}{p^e} = \tbinom{n-1}{p^e-1} \ \textit{mod } p \tag{(3)}$$

Proof. G acts on the set $\mathcal{P}$ of p^e-element subsets of G by right multiplication. One then obtains for some $P \in \mathcal{P}$ that $\bigcup P[\mathrm{stab}_G P] = P$ is a disjoint union of right cosets of $\mathrm{stab}_G P$ yielding that $\mathrm{stab}_G P \,|\, |P| = p^e$. Moreover, $P \in \mathcal{P}$ is a subgroup of G if and only if $\mathrm{stab}_G P$ has order p^e. This can be shown by the following.

If P is a subgroup then $\mathrm{stab}_G(P) = P$ since by the previous argument $\mathrm{stab}_P \subseteq P$ and P stabilizes itself. On the other hand, if $\mathrm{stab}_G P$ has the desired cardinality it follows that $\mathrm{stab}_G P = P$ since both have cardinality p^e and the first is contained in the latter. Thus P is a subgroup of G in this case.

We now obtain by orbit-stabiliser theorem

$$|\mathcal{P}| = \binom{n}{p^e} \quad = \textstyle\sum_k |\mathrm{orb}_G P_k| = \sum_k |G/\mathrm{stab}_G P_k| \tag{(4)}$$

$$= m(pl + |\mathcal{P}| \cap \mathrm{Sub}\, G) \tag{(5)}$$

for some number $l \in \mathbb{N}$ as only the G-orbits of subgroups $P \in \mathcal{P}$ have cardinality not divisible by p and the cardinality of any G-orbit is divisible by m (as we have seen above). Thus we get that

$$S_{p^e}(G) \equiv \frac{1}{m}\binom{n}{p^e} = \binom{n-1}{p^e-1} \bmod p. \tag{(6)}$$

□

Another interesting general result concerning congruences modulo p of the last type is the following

Theorem 0.3 (Lucas). *Let $m, n^j \in \mathbb{Z}$, $n = (n^j)_{j=1}^l$ be a multiindex and p be a prime. Morover let $[m]_p = m_k \cdots n_0$, $\left[n^j\right]_p = n_k^j \cdots n_0^j$ be the base p expansions of m and n^j, respectively. Then*

$$\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i} \ mod\ p \tag{(7)}$$

Proof. We have that

$$\sum_{i=1}^{l} X_j^{\ m} = \left(\sum_{j=1}^{l} X_j\right)^{\sum_{i=0}^{k} m_i p^i} = \prod_{i=0}^{k} \left(\sum_{j=1}^{l} X_j^{p^i}\right)^{m_i}$$

in $\mathbb{Z}/p\mathbb{Z}$ since the frobenius homomorphism $x \mapsto x^p$ is the identity (the X_j are variables). Comparing the coefficients before $X^n = \prod_{j=1}^{l} X_j^{n^j}$ leeds to the desired result. □

Theorem 0.4 (Sylow subgroups). *Let G be a finite group of order $n = mp^e$ with p prime $e, m \in \mathbb{N}$ and $p \not| m$. Then the number of p-Sylow-subgroups $S_{p^e}(G)$ satisfies*

$$|S_{p^e}(G)| \equiv 1 \ mod\ p \tag{8}$$

$$|S_{p^e}(G)|\,|m \tag{9}$$

$$|S_{p^e}(G)| = |G/\mathrm{N}_G(P)| \tag{10},$$

where $P \in S_{p^e}$. Moreover, they are all conjugate to each other.

Proof.

(8)arabic14: By Lucas' theorem we have that $\binom{mp^e}{p^e} \equiv \binom{m}{1} \bmod p$ proving the first fact.

□

4 Group actions

Definition 0.23. Let G be a group and Ω be an algebra (or a set). We call a homomorphism $h : G \to \mathrm{Aut}(\Omega)$ a G-action on Ω. Moreover, we call it a leftaction if $\omega^{h(g)}$ is denoted by ωg and a rightaction if it is denoted by $g\omega$.

Lemma 0.16 (orbit-stabiliser for transitive actions). *Let G act on Ω transitively und let $H \leq G$ such that H contains the stabiliser of a point $\omega \in \Omega$ and acts transitively on Ω. Then $H = G$.*

Proof. Let $g \in G$ then there exists $h \in H$ such that $\omega g = \omega h$ and thus $\omega g h^{-1} = \omega$ whence $gh^{-1} \in \mathrm{stab}_G(\omega) \leq H$. Thus $g \in H$. □

Lemma 0.17 (orbit-stabiliser for primitive actions). *Let G act on Ω transitively. The the following are equivalent:*

(I) *G acts primitively on Ω.*

(II) *When $S := \mathrm{stab}_G(\omega)$ for some point $\omega \in \Omega$. Then S is a maximal subgroup of G.*

Proof.

$(I)arabic14 \Rightarrow (II)arabic14$: Assume that $H \geq S$. Then $\{\omega Hg : g \in G\}$ is a G-invariant partition of Ω since $\omega Hg \cap \omega Hg'$ implies that there is a $h, h' \in H$ such that $h'g'(hg)^{-1} \in \mathrm{stab}_G(\omega) = S \leq H$. This implies that $g'g^{-1} \in H$ or in other words $Hg = Hg'$. It thus follows that either ωHg is a singleton or $\omega Hg = \Omega$ as G acts primitively on Ω (for all $g \in G$). In the first case we have that $\omega H = \{\omega\}$ and thus $H \leq S$ implying that $H = S$. In the second case we have that H acts transitively on Ω and thus $G = \langle H, S\rangle = HS = SH$. However, since $H \geq S$ we have that $HS = H = G$.

$(II)arabic14 \Rightarrow (I)arabic14$: If S is maximal and $\sim \subseteq \Omega^2$ is a non-trivial congruence relation (G-invariant) then for we have that $H := \mathrm{stab}_G(\omega/\sim) \neq 1$, since $\omega/\sim$ is not a singleton and G acts transitively. Thus it follows that $H \not\leq S$ and thus $\langle H, S\rangle = G$ by maximality of S in G. But since $\omega \in \omega/\sim \, \cap H \, \omega/\sim$ it follows that $S \leq H$ and thus $H = G$. But then $\mathrm{orb}_H(\omega) = \omega/\sim \, = \Omega$ since $G = H$ acts transitively. Thus G must act primitively on Ω.

□

Lemma 0.18. *Let G act on Ω via $\alpha : G \to \mathrm{Aut}(\Omega)$ and $N \trianglelefteq G$. Then G/N acts on Ω/N via $\overline{\alpha} : G/N \to \mathrm{Aut}(\Omega/N)$ where $(\omega N)(gN) := (\omega g)N$.*

Proof. We have to show that the action is welldefined. This follows from $NgN = gN^gN = gN$. □

False:

Lemma 0.19 (characterisation of primitive actions). *Let G act faithfully on Ω. The following are equivalent*

(I) *Any normal subgroup $N \neq 1$ of G acts transitively on Ω.*

(II) *Any minimal normal subgroup of G acts transitively on Ω.*

(III) *G acts primitively on Ω.*

Proof.

$(III)arabic15 \Leftrightarrow (I)arabic15$: Let $N \trianglelefteq G$ and let G act on Ω primitively via $\phi : G \to \mathrm{Aut}(\Omega)$. Then G acts on Ω/N via $G \to G/N \to \mathrm{Aut}(\Omega/N)$. Thus it follows that $\Omega/N = \Omega$ or $\Omega/N = \{\{\omega\} : \omega \in \Omega\}$ as G acts primitively on Ω. In the first case we have that N acts transitively on Ω and in the second case we have that $N = 1$ since for all $n \in N$ it then holds that $\alpha(n) = \mathrm{id}_\Omega$

which implies by primitivity of the action of G (i.e. injectivity of α) that $N = 1$. Conversely, if $\Omega/\sim \subseteq \operatorname{Sub}\Omega$ is a system of imprimitivity, then we have $G \to \operatorname{Aut}(\Omega) \to \operatorname{Aut}(\Omega/\sim)$ where the last arrow is induced by the natural projection map $\pi : \Omega \to \Omega/\sim$ with $\omega \mapsto \omega/\sim$. But as $\sim$ is not a trivial congruence we have that $\operatorname{Aut}(\pi)$ has as a kernel a normal subgroup $N \trianglelefteq \operatorname{Aut}(\Omega)$ with $1 < N < \operatorname{Aut}(\Omega)$. Thus $1 < N \wedge \operatorname{im}(\alpha) \trianglelefteq \operatorname{im}(\alpha)$. To be continued.

$(I)arabic15 \Leftrightarrow (II)arabic15$: If any normal subgroup N of G acts transitively then especially every minimal one does. Conversely, any normal N subgroup contains a minimal normal subgroup $M \trianglelefteq G$. Thus N must act transitively if any minimal normal subgroup does.

□

Corollary 1. Let G act primitively on Ω and let $N \trianglelefteq G$. Then N acts transitively on Ω.

Lemma 0.20 (Dedekind's medular law). *Let $J, K, L \leq G$ be groups and $J \leq L$. Then it holds that*

$$J(K \wedge L) = JK \wedge L. \tag{(11)}$$

Proof.

$\supseteq$: We have that $J(K \wedge L) \leq J(JK \wedge JL) \leq JK \wedge L$.

$\subseteq$: If $j \in J, k \in K$ such that $jk \in L$, then $k \in j^{-1}L = L$ (since $J \leq L$). Thus $jk \in J(K \wedge L)$.

□

Lemma 0.21 (join with normal subgroup). *Let $H, N \leq G$, $N \trianglelefteq G$. Then $H \vee N = HN = NH$. If $H \wedge N = 1$ then $H \wedge N \Leftrightarrow H \ltimes N$.*

Proof. Of course we must have $HN \leq H \wedge N$. As N is normal we have $nh = h(h^{-1}nh) = hn^h \in HN$ which shows that $NH = HN$ and thus $(HN)^2 = H^2N^2 = HN$ and $(HN)^{-1} = N^{-1}H^{-1} = NH = HN$ showing that HN is already a group, thus $HN = NH = H \wedge N$.

If $H \wedge N = 1$, it follows that any element $g = hn \in HN$ with $h \in H$, $n \in N$ is unique in this representation as $hn = h'n'$ implies ${h'}^{-1}h = n'n^{-1} \in H \wedge N = 1$. Moreover, H acts on N via $\alpha : H \to \operatorname{Aut}(N)$ with $n^{\alpha(h)} := h^{-1}nh$. Thus $\phi : H \ltimes_\alpha N \to HN$ with $(h, n) \mapsto hn$ is an isomorphism of groups since $\phi((h, n)(h', n')) = \phi((hh', n^{h'}n')) = hh'n^{h'}n' = hnh'n' = \phi(h, n)\phi(h', n')$ and ϕ is bijective (as outlined before). □

Lemma 0.22 (third isomorphism theorem, projection law). *Let $H, N \leq G$ be groups and $N \trianglelefteq H \vee N$ (that is $H \leq \mathrm{N}_G(()N)$). Then $H \wedge N \trianglelefteq H$ and*

$$(H \vee N)/N = HN/N \Leftrightarrow H/(H \wedge N). \tag{(12)}$$

Proof. We have that $N^h = N$ for all $h \in H$ thus $(N \wedge H)^h = N \wedge H$ for all $h \in H$. Thus $H/(H \wedge N)$ is well defined and one easily verifies that $h(H \wedge N) \mapsto hN$ is an isomorphism with inverse $hN \mapsto hN \cap H$. □

Remark 1. The third isomorphism theorem for groups is basically a consequence of the more general version in universal algebra.

Lemma 0.23 (Gauss). *Let q be an odd prime power and $a \in {\mathbb{F}_q}^*$. Show that $x^2 = a$ has a solution in x if and only if $a^{\frac{q-1}{2}} = 1$.*

Proof. If ξ is generator of $(\mathbb{F}_q)^*$ then $a = \xi^n$ for some $n \in \{0, \ldots, q-2\}$ we have $a = \xi^n$ and $q - 1 | n\frac{q-1}{2}$. Thus $2|n$ and we find the solutions $\pm\xi^{n/2}$. Conversely, when $a = x^2$ then $a^{\frac{q-2}{2}} = x^{q-1} = 1$. □

Exercise 0.6. Let p, q odd primes with $p \neq q$. How many solutions x has the equation $x^2 = a \neq 0$ which are themselves a square if a is a square.

Solution. When ξ is a generator of $(\mathbb{F}_q)^*$ then some solution $\mod p$ is ξ^n and the other is $\xi^{n+\frac{p-1}{2}}$. If $p \equiv 1 \bmod 4$ then both exponents are even or odd. Otherwise, one is even and one is odd. The same holding for q one sees that there is exactly one square x satisfying the equation if $p \equiv q \equiv 3 \bmod 4$, two or zero such x if $p \not\equiv q \bmod 4$ and zero or four such x if $p \equiv q \equiv 1 \bmod 4$.

14 Ring theory

Lemma 0.24 (quotient prime ideal). *Let R be a commutative ring and $\mathfrak{p} \in \operatorname{con}(R)$. Then the following two are equivalent*

(I) $R/\mathfrak{p}$ is an integral domain.

(II) $\mathfrak{p}$ is a prime ideal.

Proof.

$(II) arabic17 \Rightarrow (I) arabic17$: Let $\overline{a}, \overline{b} \in R/\mathfrak{p}$ such that $\overline{a}\overline{b} = 0$. Then it follows that $ab \in \mathfrak{p}$ and thus as $\mathfrak{p}$ is a prime ideal that $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. But this implies that $\overline{a} = 0$ or $\overline{b} = 0$.

$(I) arabic17 \Rightarrow (II) arabic17$: When $R/\mathfrak{p}$ is an integral domain and $\overline{a}, \overline{b} \in \operatorname{con}(R)$ such that $\overline{a}\overline{b} = 0$ then $\overline{a} = 0$ or $\overline{b} = 0$ or equivalently $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

□

Lemma 0.25 (quotient maximal ideal). *Let R be a commutative ring and $\mathfrak{m}$ an ideal. Then the following two are equivalent*

(I) $R/\mathfrak{m}$ is a field.

(II) $\mathfrak{m}$ is a maximal ideal.

Proof.

$(I)arabic17 \Rightarrow (II)arabic17$: When $R/\mathfrak{m}$ is a division ring and $a \notin \mathfrak{m}$ then $\overline{a} \neq 0$ so it is a unit. Thus $\langle \overline{a} \rangle = \overline{a}R/\mathfrak{m} = R/\mathfrak{m}$ implying that $\langle \mathfrak{m}, a \rangle = R$ so $\mathfrak{m}$ is maximal.

$(II)arabic17 \Rightarrow (I)arabic17$: When $\mathfrak{m}$ is maximal and $0 \neq \overline{a} \in R/\mathfrak{m}$ then $a \notin \mathfrak{m}$ meaning that $\langle a, \mathfrak{m} \rangle = aR + \mathfrak{m} = R$ as $\mathfrak{m}$ is maximal. This implies that there exist $b \in R$ such that $ab + \mathfrak{m} = 1 + \mathfrak{m}$. Thus $\overline{b}$ is the inverse of $\overline{a}$ in $R/\mathfrak{m}$.

□

Lemma 0.26. *Let $\mathfrak{m} \in \mathrm{con}(R)$ be a maximal ideal of a commutative ring R. Then $\mathfrak{m}$ is a prime ideal.*

Proof. Let $a, b \in R$ with $ab \in \mathfrak{m}$. Assume that $a, b \notin \mathfrak{m}$ then $aR + \mathfrak{m} = bR + \mathfrak{m} = R$ so $abR + a\mathfrak{m} + b\mathfrak{m} + \mathfrak{m}\mathfrak{m} = R \leq \mathfrak{m}$ a contradiction. □

15 Partial fractions

Lemma 0.27 (partial fraction representation, principal ideal domain). *Let R be a principal ideal domain and let $Q := \mathrm{Q}(R)$ its quotient field. Then any element of $f = f_0(\prod_{i=1}^{n} p_i^{\nu_i})^{-1} \in Q$ ($f_0, p_i \in R$, $f_0 \wedge p_i = 1$, $\nu_i > 0$, $i = 1, \ldots, n$) can be written as*

$$f = \sum_{i=1}^{n} \frac{a_i}{p_i^{\nu_i}}$$

where $a_0, a_i \in R$ and $a_i \wedge p_i = 1$ ($i = 1, \ldots, n$).

Proof. The proof is given by the fact that

$$\bigvee_{i=1}^{n} \left\langle \prod_{j \neq i} p_j^{\nu_j} \right\rangle_{\mathrm{con}} = R = \langle 1 \rangle_{\mathrm{con}}$$

since R is a factorial domain whence prime elements p_i are also irreducible. Interpreting this equation in the fractional field and multiplying by $\prod_{i=1}^{n} p_i^{\nu_i}$ we get the desired fact since in a PID

$$\bigvee_{i=1}^{n} \mathfrak{a}_i = \sum_{i=1}^{n} \mathfrak{a}_i.$$

□

Remark 2 on uniqueness. Note that there is no statement about uniqueness of the partial fraction representation in PIDs. In fact, it is immediately clear that without an additional restriction the above representation is not unique in most cases. But the image $\overline{a_i}$ under the natural map $\pi_i : R \to R/\langle p_i^{\nu_i} \rangle_{\mathrm{con}}$ is unique for $i = 1, \ldots, n$. This can be seen by multiplying the partial fraction

representation by $\prod_{i=1}^{n} p_i^{\nu_i}$ and then taking the image under the above map (modulo $p_i^{\nu_i}$). This yields $\pi_i(\prod_{j\neq i} p_j^{\nu_j} a_i)$. But since R is an integral domain and p_j, p_i coprime for $i \neq j$, this already uniquely determines $\pi_i(a_i) = \overline{a_i}$.

In most cases we deal with polynomials when talking about partial fractions.

Lemma 0.28. *Let $p, q \in K(X)$ be coprime for an algebraically closed field K.*

$$p/q =$$

and the a_{ij} are given by the formula

16 Ordered monoids and metric spaces

Definition 0.24 (ordered monoid). A structure $A = \langle M, 1, \cdot, \leq \rangle$ where $\langle M, 1, \cdot \rangle$ is a monoid and $\leq \subseteq M \times M$ is an order being compatible with the multiplication, i.e.

$$\leq \in \mathrm{Inv}(\cdot)$$

or explicitely

$$(a \leq b) \wedge (c \leq d) \Rightarrow (ac \leq bd) \wedge (ca \leq db).$$

If 1 is minimal in M we say that M is an *upright monoid*.

Definition 0.25 (ideal in an upright monoid). Let A be an upright monoid. Then a subset $\mathfrak{b} \subseteq A$ is called an order ideal if $A\mathfrak{b} = \mathfrak{b}A = \mathfrak{b}$ (absorbative), $a\mathfrak{b} = \mathfrak{b}a$ (normal) and it holds that $a \leq b \Rightarrow a \in \mathfrak{b}$ (absorbative in order sense) for $b \in \mathfrak{b}$, $a \in A$.

Lemma 0.29 (representation of the generated ideal). *Let $B \subseteq A$ a set. Then the upright ideal generated by B is $\bigcup_{n\in\mathbb{N}} (AB)^n$.*

Lemma 0.30 (first homomorphism theorem for upright monoids). *Let $h : A \to B$ be a homomorphism of ordered monoids then $\ker h = h^{-1}[0]$ is an ideal. Moreover, $A/\ker h \Leftrightarrow \operatorname{im} h$*

Proof. Clearly, when $a \in A$, $b \in \ker h$ we have that $ab, ba \in \ker h$ since $h(ab) = h(ba) = h(b) = 1$. Moreover, when $a \leq b$ (for the same a and b), then $h(a) \leq h(b) = 1$ implying that $h(a) = 1$ since 1 is minimal. The rest follows by general isomorphism theorem. □

Definition 0.26 (unit in upright monoid). Let A be an upright monoid and $a \in A$. Then a is called a *order unit* if $\langle a \rangle_{\mathrm{con}} = A$ (unit if also unit in the monoid sense). We write $A^\times$ for all these elements of A.

Remark 3. The units $A^\times$ form a monoid as for $a, b \in A^\times$ we have $ab = aAb = \ldots$

Definition 0.27 (A-metric space). An A-metric space where A is an upright abelian monoid is a structure $M = \langle S, d \rangle$ where S is a structure which bases on

Set and $d : S \times S \to A$ satisfies

$$d(a,b) \leq d(a,c) + d(c,b), \tag{(13)}$$
$$d(a,b) = d(b,a), \tag{(14)}$$
$$d(a,a) = 0. \tag{(15)}$$

for $a, b, c \in M$.

Lemma 0.31 (Lebesgue). *Let K be a compact A-metric space and $\mathcal{U}$ be an open cover of K, i.e. $\bigcup \mathcal{U} = K$. Then there exists an $\varepsilon > 0$ such that for any $k \in K$ the ball $\mathbb{B}_\varepsilon(k)$ lies entirely in some set $U \in \mathcal{U}$.*

Proof. Define $\mathcal{U}' := \{\mathbb{B}_\varepsilon(k) : \varepsilon > 0 \wedge \exists U \in \mathcal{U} : \mathbb{B}_{2\varepsilon}(k) \subseteq U\}$. Then $\mathcal{U}'$ also covers K since for $k \in K$ there is a $U \in \mathcal{U}$ with $k \in U$ and U is open in k. Now, choose a finite subcover $\mathcal{F}$ of $\mathcal{U}'$. Then there exists a minimal radius ε among the balls in $\mathcal{F}$. Now, for all balls $\mathbb{B}_\varepsilon(k)$ in $\mathcal{U}$ we find a ball $\mathbb{B}_\varepsilon(k') \in \mathcal{F}$ containing k. This means that $\mathbb{B}_\varepsilon(k) \subseteq \mathbb{B}_{2\varepsilon}(k')$. But for this last ball we know by the definition of $\mathcal{U}$ that it is enterily contained in some set $U \in \mathcal{U}$. This shows that the desired for this $\varepsilon > 0$. □

Lemma 0.32 (sequencial compactness).

Proof. Let $\mathcal{U}$ be an open cover of M such that $\mathcal{U}$ has no finite subcovers. By the previous lemma, we know that there is a number $\varepsilon > 0$ such that the cover $\mathcal{U}' := \{\mathbb{B}_\varepsilon(k) : k \in K\}$ has the property that for any ball $B \in \mathcal{U}'$ there exists $U \in \mathcal{U}$ such that $B \subseteq U$. Thus $\mathcal{U}'$ cannot have a finite subcover, too, since otherwise $\mathcal{U}$ would admit one. From this we see that there is a sequence of balls $(\mathbb{B}_\varepsilon(k_n))_{n\in\mathbb{N}}$ of $\mathcal{U}'$ such that $k_n \notin \mathbb{B}_\varepsilon(k_i)$ for $i < n$. But then the sequence $(k_n)_{n\in\mathbb{N}}$ cannot have a convergent subsequence since the distance between any two distinct points of it is at least ε. Thus M is not sequencially compact. □

17 Euclidean geometry

Isoperimetric inequality in two dimensions. Lemma 0.33. *Among all Jordan curves C in the plane of a given length circles enclose the largest area.*

Proof. Let C be a jordan curve of finite length then $\partial\mathrm{conv}\, C$ is a curve of at most the length of C prescribing at least the area inside C. Thus we may assume that C is the boundary of convex set (and thus differenciable nearly everywhere). For point $x, y \in C$ we then may choose points w, z such that $xwyz$ is a kite. We can than modify that kite leaving its side length fixed such that its area is maximal moving the bows of C above the sides of $xwyz$ with them. This clearly happens when $\angle zxw = \angle wyz = \pi/2$. ... From this one gets that any three points of C lie on a circle. □

Lemma 0.34 (Steiner's equations). *Let $P \subseteq \mathbb{R}^n$ be a convex polytope. Then it holds that*

$$\mathrm{vol}_{\mathbb{R}^n}(P + \varepsilon\mathbb{B}^n) = \mathrm{vol}_{\mathbb{R}^n}(P) + \sum_{i=1}^{n} \varepsilon^i \sum_{f \in F_i(P)} \mathrm{vol}_{\mathbb{R}^{n-i}}(f) \frac{\mathrm{vol}_{\mathbb{S}^i}(\alpha_f)}{i}$$

and

$$\mathrm{vol}_{\mathbb{R}^n}\left(\partial(P+\varepsilon\mathbb{B}^n)\right)=\sum_{i=1}^{n}\varepsilon^{i-1}\sum_{f\in F_i(P)}\mathrm{vol}_{\mathbb{R}^{n-i}}(f)\,\mathrm{vol}_{\mathbb{S}^i}(\alpha_f)=\left.\frac{\partial\mathrm{vol}_{\mathbb{R}^n}(P+\mathbb{B}_r)}{\partial r}\right|_{\varepsilon},$$

where $F_i(P)$ means the i-dimensional faces of P and α_f means the spherical polytope associated to the face f.

Lemma 0.35 (sum of exerior angles of convex polytope). *For a convex polytope $P\subseteq\mathbb{R}^n$ it holds that*

$$\sum_{f\in F_{n-1}(P)}\alpha_f=\mathbb{S}^n$$

(in the sense of elementary geometric addition).

Corollary 2 (isoperimetric inequality for convex polytopes). Let P be a convex polytope then

$$\frac{\left(\mathrm{vol}_{\mathbb{R}^{n-1}}(\partial P)\right)^n}{\left(\mathrm{vol}_{\mathbb{R}^n}(P)\right)^{n-1}}\geq\frac{\left(\mathrm{vol}_{\mathbb{R}^{n-1}}(\mathbb{S}^{n-1})\right)^n}{\left(\mathrm{vol}_{\mathbb{R}^n}(\mathbb{B}^n)\right)^{n-1}}.$$

Proof. We may assume

$$\frac{\mathrm{vol}_{\mathbb{R}^{n-1}}(\partial P)}{\mathrm{vol}_{\mathbb{R}^n}(P)}=\frac{\mathrm{vol}_{\mathbb{R}^{n-1}}(\mathbb{S}^{n-1})}{\mathrm{vol}_{\mathbb{R}^n}(\mathbb{B}^n)}=n.$$

as the inequality is invariant under scaling P by scalars.

Interpolation between P and the n-ball know leads to

$$\frac{\mathrm{vol}_{\mathbb{R}^n}\left(\partial(P+\varepsilon\mathbb{B}^n)\right)}{\mathrm{vol}_{\mathbb{R}^n}\left(P+\varepsilon\mathbb{S}^{n-1}\right)}=$$

□

Lemma 0.36. *Let X be a topological space and $\mathcal{C}(X)$ be the topological space defined by $\mathcal{C}(X):=\{Y\subseteq X:Y$ is compact$\}$ equipped with the topology $\tau_{\mathcal{C}(X)}:=\{\{x\in\mathcal{C}(X):x\subseteq U\}:U\in\tau_X\}$.*

TEST:
where $\mathrm{pr}_i\circ\mathrm{incl}_j=\pi_i\circ\iota_j=\delta_{ij}$

18 *

Index

sd

Test. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.